

(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 022 638 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

26.07.2000 Bulletin 2000/30

(51) Int. Cl.⁷: G06F 1/00

(21) Application number: 00100476.1

(22) Date of filing: 11.01.2000

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(72) Inventors:

• Hansmann, Uwe

71155 Altdorf (DE)

• Seliger, Frank

71157 Hildrizhausen (DE)

(30) Priority: 12.01.1999 EP 99100474

(71) Applicant:

International Business Machines Corporation
Armonk, NY 10504 (US)

(74) Representative:

Teufel, Fritz, Dipl.-Phys. et al

IBM Deutschland Informationssysteme GmbH,

Intellectual Property,

Pascalstrasse 100

70548 Stuttgart (DE)

(54) **Method and system for securely handling information between two information processing devices**

(57) Described is a mechanism for securely handling an information unit by a first information processing device (2), for instance a terminal device like a chip card reader, which interoperates with a second secure information processing device (1), for instance a portable device like a chip card, whereby the information unit is provided by an issuer. The information unit is provided from the issuer to the first device and encrypted by using a first key. The first key is also encrypted by using a second key. The second key is provided on the second secure device (1) and interconnecting the first and the second device enables to decrypt the first key by using the second key and then to decrypt the information unit by using the first key.

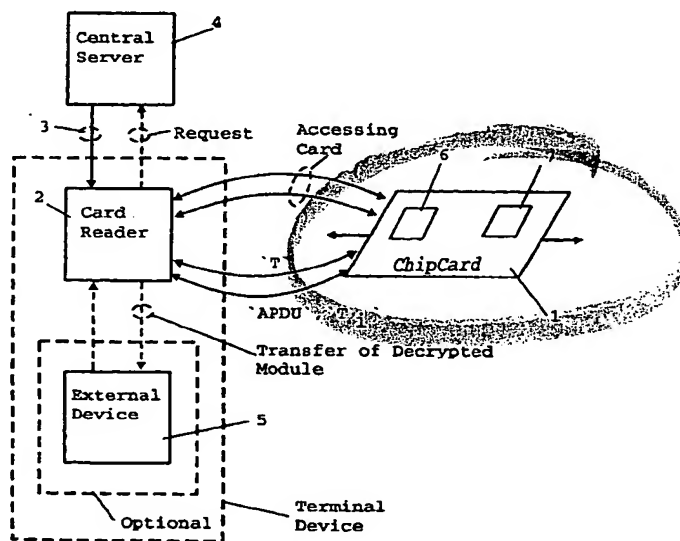


FIG. 1

BEST AVAILABLE COPY

EP 1 022 638 A2

Description

[0001] The invention generally relates to secure interoperation between two information processing devices where only one of these devices can handle information in a secure manner. In particular, the invention relates to a method and a system for securely handling an information unit by a first information processing device, for instance a terminal device, inter-operating with a second secure information processing device, for instance a portable device like a chip card, whereby the information unit is provided by an issuer.

[0002] It is commonly known that chip cards are not only utilized as a memory for storing data on it but also used as an access control medium or a medium to enable and perform encryption and decryption of information. Therefore, from the beginning of development of chip cards, the field of cryptology has played a central or even dominant role. Meanwhile, the scientific results of this development field are inseparably related to chip card technology.

[0003] The technical field of cryptology divides into two fields of activity, namely cryptography and cryptanalysis. The field of cryptography embraces the science and methodology of encryption and decryption of information. The science of cryptanalysis addresses to crack existing cryptographic systems.

[0004] In the field of chip card technology, another major issue is practicability of the scientific and theoretical aspects of cryptology.

[0005] The predominant objective of cryptology is, on the one hand, secrecy of information and, on the other hand, securing or safeguarding the authentication of information. Both objectives are independently of each other and thus have different requirements of the respective information system. 'Secrecy' means that only the addressed receiver is able to decrypt the contents of a message. In contrast to that, 'authenticity' enables the receiver of the message to secure that the received message has not been altered during transmission.

[0006] For the following description of known techniques of data encryption/decryption it is referred to chapter 4 of the "Handbuch der Chipkarten", W. Rankl, W. Effing, 1996, Hauser Verlag, Munich-Vienna, which contents are regarded to be fully incorporated herein. Each encryption technique uses three types of information. Non-encrypted data are designated as "plain text" wherein encrypted data are designated as "cypher text". For encryption/decryption one or more keys are required as a third type of data. All these types of data are to be processed by an encryption algorithm. Cryptographic algorithms currently used in chip cards are generally block-oriented, which means that the plain text and the cypher text are always processed as packages of a given length, e. g. 8 byte in case of the algorithm used by the decryption/encryption standard (DES) which is discussed in more detail in the following.

[0007] It is emphasized hereby that the present invention is applicable to all described fields of cryptography like encryption, decryption, or one-way cryptographic functions like hash values or a digital signature verification mechanism. Modern cryptographic algorithms are generally based on the known Kerckhoff principle which says that the entire security of an algorithm shall only depend on secrecy of the underlying keys, but not on secrecy of the cryptographic algorithm itself.

[0008] Besides Kerckhoff, a further known principle is security through masking which presumes that a fictitious attacker does not know how the system works. But the latter principle is by no means sufficient to secure an information handling system. The security of modern and already published cryptographic algorithms does, in practice, only depend on the performance of the computers used to crack a cryptographic algorithm and thus an alleged additional masking technique of the utilized methodology of cryption one achieves a considerably increased protection against attacks. Otherwise, the rapidly progressing development of computer performance causes a doubling of performance within about one and a half years and thereupon the increasing number of participants of the worldwide computer network, e. g. the WEB, provide a further way to perform serious attacks on cryptographic systems or related keys.

[0009] In order to crack a cryptographic algorithm, there are different ways of attacks. A first one is the "cypher text only attack" where the attacker does only know the cypher text and tries to obtain the key or plain text by use of this information. A more promising attack is the so-called "known plain text attack" where the attacker is in the possession of a number of plain-text/cypher-text pairs for a secret key. The secret key can be obtained by trial and error. The most trivial attack is to find out the secret key only through trial and error which is called "Brute force attack". By using a large performance computer, on the basis of a known plain-text/cypher-text pair, all feasible encryption keys are tried until the right one is obtained. The teaching of statistics says that on an average only the half of all possible keys has to be checked in order to find the right one. For that reason, a large space of possible keys renders that kind of attack more difficult.

[0010] Cryptographic algorithms are further divided into symmetric and asymmetric algorithms, dependent on the respectively utilized key. 'Symmetric' means that the algorithm for en- and decryption is using the same key. In contrast to that, 'asymmetric' cryptographic algorithms, like that proposed by Whitfield Diffie and Martin E. Hellman in 1976, are using different keys for encryption and decryption. The two major principles for a well performing encryption algorithm are the principles of 'confusion' and 'diffusion' after C. Shannon. It is emphasized that both types of algorithms can be taken as a basis for the present invention.

[0011] Symmetric cryptographic algorithms are

based on the principle of utilizing the same key for both encryption and decryption. A well-known data encryption algorithm called 'Data Encryption Algorithm' (DEA) has been proposed by the applicant of the present application together with the U.S. National Bureau of Standards developed in 1977. This standard algorithm is often be referred to as 'Data Encryption Standard' (DES). Since that algorithm is designed in consideration of Kerckhoff's dogma, it could be published without any impact on its security. For the details of that algorithm it is further referred to National Institute of Standards and Technology (NIST), FIPS Publication 46-2, "Data Encryption Standard", December 1993.

[0012] The principle of 'confusion' means that the statistics of the cypher text shall influence the statistics of the plain text so that an attacker can not take profit by that. The second principle "diffusion" means that every bit of the plain text and of the key shall influence as much bits of the cypher text as possible.

[0013] The DEA is a symmetric encryption algorithm using block architecture. It does not perform expansion of the cypher text which means that plain text and cypher text are of identical length. The block length is 64 bit (= 8 byte), the key is also 64 bit long but includes 8 parity bits whereby the available space of possible keys is considerably reduced which is in case of DES $2^{56} = 7,2 \times 10^{16}$ possible keys. But in view of the continuously and permanently increasing computer performance such a space of possible keys is regarded as the lower limit for the required security of a cryptographic algorithm.

[0014] As an exemplary asymmetric cryptographic algorithm, it is referred to the one proposed by Whitfield Diffie and Martin E. Hellman, published in 1976, which is based on two different keys. One of these keys is public, the other is secret. An information or message is encrypted by using the public key prior to transmission of an information and only the owner of the secret key is enabled to decrypt again the encrypted message. In particular, that principle for the first time enables implementation of a digital signature which in principle can be verified by everyone who is in the possession of the required (public) key. Exemplarily, it is referred to a first implementation of the prementioned principle for asymmetric cryptographic algorithms, namely the 'RSA' algorithm proposed by Ronald L. Rivest, Adi Shamir and Leonard Adleman which is the currently best known and most versatile asymmetric cryptographic algorithm. Its functional principle is based on the arithmetic of big integer numbers. Both keys are generated based on two big prime numbers. Encryption and decryption can be mathematically expressed by a modulo function, namely in case of encryption $y = x^e \bmod n$, for decryption $x = y^d \bmod n$ with $n = p \times q$ wherein x = plain text, y = cypher text, e = public key, d = secret key, n = public modulus and p, q = secret prime numbers.

[0015] For the further details of an implementation of the RSA algorithm it is accordingly referred to R. L.

Rivest, A. Shamir, and L. M. Adleman "A Method for obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21(2), pages 120 - 126, February 1978.

[0016] In addition to secrecy of information, another paradigm for encryption algorithms is 'authenticity' of a received message or information. As mentioned above, authenticity means that a message is not altered e. g. not manipulated. For that purpose, to the actual message a message authentication code is appended and both parts are transmitted to the receiver. The receiver is enabled to calculate its own message authentication code (MAC) and compares that code with the received code. In case of both matching, it is secured that the transmitted message has not been altered during transmission. For generating a MAC, a cryptographic algorithm with one secret key which is known to both communication partners is utilized. For the calculation of a MAC in principle every cryptographic algorithm can be used, but in practice, the above mentioned DEA algorithm is utilized nearly exclusively.

[0017] A particular scenario for the present invention is a situation where a chip card is inserted in a chip card acceptance device - in the following called "terminal device" - which does not yet have a support module capable of accessing the card or to fulfill a particular function of the chip card on the terminal. Therefore it is required to obtain the missing software component from an other source of information e. g. to download such required module from a central server connected to the internet. It is noted that the terminal device can either be a computer, like a personal computer or network computer with a chip card reader/writer hardware, or a specialized device combining the chip card reader/writer hardware with an embedded computer.

[0018] The transmission will often take place over a network that is open to attacks. It is known that the chip card hereby ensures that the software component in the device accessing the chip card shares a secret to the chip card by using mechanisms called external authentication or challenge/response. Further, it is known that a digital signature secures the download of software but the public keys of all potential senders have to be stored on the hard disk of the computer. Therefore, it is necessary that it can be ensured that the software was not altered on its way through the network and that the software was sent by the owner of the public key. But getting the public key for signature verification must also be done in a secure way, before the download is secure. This requires a chain of certification authorities.

[0019] On the other hand, an authentication mechanism is needed to verify that the obtained software component is the most recent issued release of that software. Today, the version control is handled by continuously increasing a version number.

[0020] It is therefore an object of the present invention to provide a method and a system for securely inter-operating a first information processing device, in

particular a terminal device like a chip card reader, and a second secure information processing device, in particular a portable device like a chip card, where the first device does not yet have an information unit like a software component required for interoperating the first and the second device like providing or controlling access to the second secure device. It is therefore required that the missing information unit is obtained from an other source of information. A particular object of the invention which is strongly related to the above object is that gathering the missing information unit is to be accomplished in a secure manner.

[0021] In order to solve the above objects and to avoid the above-mentioned drawbacks of existing mechanisms and systems, the invention proposes that the information unit is provided from the issuer to the first information processing device whereby the information unit is processed by a cryptographic process i.e. for instance encrypted and/or signed by a signature. The required key for the cryptographic process is particularly provided on the second secure information processing device. The information unit is cryptographically reprocessed i.e. for example decrypted and/or its signature verified by using the key. It is emphasized that the information unit can be secured by alternatively using encryption/decryption and signature verification or by using both mechanisms in parallel.

[0022] According to a first preferred embodiment, the information unit is provided from the issuer to the first information processing device whereby the information unit is encrypted by using a first key which is also provided in an encrypted format by using a second key. The second key is provided on the second secure information processing device and interconnecting the first information processing device and the second secure information processing device therefore enables to decrypt the first key by using the second key. By using the decrypted first key, the information unit can also be decrypted.

[0023] According to a second preferred embodiment of the invention, the information unit is provided from the issuer to the first information processing device whereby the information unit is signed by using a signature. The signature is provided from the issuer to the first information processing device whereby the signature is generated by using at least one key. Further the at least one key for signature verification is provided on the second secure information processing device. After the first information processing device and the second secure information processing device have been interconnected, the at least one key for signature verification is transferred from the second secure information processing device to the first information processing device. Finally the signature of the information unit is verified by using the at least one key.

[0024] It is noteworthy that the information unit can be any set of (pure) data or an executable code like an application program or a hardware driver to run on the

second secure device and/or the other device(s), i. e. any kind of information. Further the information unit can serve to run specific functions of the second secure device on the first device or on at least a third device attached to the first device. In particular, the information unit can provide an access control for the second secure device. Further, the second secure information processing device can be any device where the issuer of that device, and of the information unit, can secure that the private key "I" is secure and not alterable, i. e. securely stored on the device. Exemplary devices are chip cards, in particular smart cards, Personal Computers with an according access control, or any other portable devices like laptops, palmtops, organizers, etc. Accordingly, the first information processing device can be any device with which the second secure device can interoperate like a card accepting device, e.g. a card reader, or even a computer with a card accepting device attached thereto.

[0025] In particular, according to the invention, the second secure device provides the second key by which the first key has been encrypted and therefore interconnecting the first, device and the second device enables firstly to decrypt the first key by using the second key and, secondly, to decrypt the information unit by using the decrypted first key. The basic concept of the invention therefore is to have the private (second) key securely stored on the second secure information processing device what guarantees that this key will remain private i. e. can not be gathered by a third party.

[0026] In case of a chip card and a chip card accepting device, the invention particularly enables dynamic secure download and execution of a missing software support, for instance support needed for specific functions of a chip card on a device attached to the chip card acceptance device. The software component can only be decrypted by the usage of a key "T". This key is transmitted in an encrypted form as key "T_i" together with the software encrypted with it. Key "T_i" can only be decrypted by the chip card knowing the key "I" that was used to encrypt the key "T". The key "I" is stored on the chip card by the issuer at the time of card issuing. One of the advantages of this procedure is that the issuer of the card can secure that the key "I" is a private key insofar as it is guaranteed that the key is not known by others. Further, any later required software support for the chip card can be secured by using this key. On the other hand, the session key "T" which maybe will be known by others through transfer to the terminal device, can be changed by the issuer from session to session thus considerably enhancing data security. To make the card decrypt key "T_i" using key "I", a command (APDU) is passed to the chip card that was transmitted together with the software module to be decrypted and used. In other words, the chip card which may be controlled by the downloaded software, itself plays a critical role in securing the integrity of the driving software. Insofar, the chip card itself retrieves the key T

which has been used to encrypt the downloaded software via decryption of the encrypted key T_i . To prevent alteration of the transmitted software module, it is proposed that it will be encrypted or signed with one of the standard algorithms described in the introductory part. The issuer of the software has the required encryption, decryption or signature keys. Instead of requiring the terminal device to store and retrieve the matching decryption key or fetch the matching certificate, the present invention describes a way of using the chip card itself to retrieve that key. The chip card advantageously is the most secure and most convenient way to store the secret decryption key or the certificate or the card issuer. In this way, only software that is certified by the card issuer should be allowed to access the card.

[0027] It is emphasized that beyond encryption/decryption the invention can also employ digital signing or digital signature verification for the encryption by using the first key and/or the second key. For this signature case, the described mechanism provides a trusted way to the issuer's public signature key without the requiring complex certificate handling including chains of trust.

[0028] The information unit can advantageously be a program module or data to control access to a portable device by the terminal device, the integrity of the information unit hereby playing a rather critical role for data security. Further, the information unit can be an application program which can run either on the portable device or the terminal device or can serve to run specific functions of the portable device on the terminal device or on a second device attached to the terminal device. Also in these cases, data integrity plays a dominant role.

[0029] Portable devices like chip cards commonly provide only limited resources for processing data and according limited space for storing data. Therefore, according to another embodiment of the invention, both the decryption of the first key and the decryption of the information unit are accomplished on the terminal device's side.

[0030] In order to provide a more powerful and automatically operating system, according to another embodiment of the invention the first device provides a control command (APDU) to the second secure device which initiates or triggers the transfer of the second key to the first device, or initiates or triggers the beginning of decryption of the first key by using the second key. Hereby an operating system or program of the first device advantageously must not know how to decrypt key " T_i " and can be freed from performing the decryption procedure. The first device only passes the APDU command to the second secure device. This embodiment enables that the entire procedure proposed by the invention can be performed in the background i. e. not visible to the user whereby in particular the required second key is transferred to the first device without any needed interaction by the user.

[0031] In a preferred embodiment of the invention, the encrypted information unit and the encrypted first key are downloaded from a central server, e.g. a server interconnected with the Internet, particularly from a server provided by the issuer of the second secure device. Alternatively, the above mentioned control command can be downloaded, too, from such a server. In view of the continuously increasing meaning of the Internet, such kind of software support via download is a preferred way to obtain a required information unit.

[0032] In a further preferred embodiment of the invention, the second key required to decrypt the first key is securely stored on the second secure device at time of its issuing by the issuer. Since the issuer of the card will often be identical with the issuer of the information unit, it is hereby guaranteed that the second key will be compatible with the encryption of the first key.

[0033] According to a further embodiment of the invention, a third key can be used for authentication or version control of the underlying information unit. Hereby the second secure device contains a version number and a key "E" which the downloaded information unit accessing the second secure device must know. To prove that the information unit has the matching key "E", a challenge/response mechanism ("external authentication") is used. This allows the issuer of the second secure device by changing the key "E" on that device, in combination with the other steps of the proposed mechanism, to initiate the second secure device and/or the first device to download a new version of the underlying information unit.

[0034] Using such a third key, it is possible to realize a further automatization of the proposed mechanism where the first device is initiated to download a new release of the information unit.

[0035] The proposed arrangement of the two different key levels enables, in accordance with another preferred embodiment of the invention, that the first key can be randomized between different sessions of interoperating the first and the second device, i. e. the issuer of the second secure device every time can use another random key T to encrypt the information unit with the cryptographic function. Therefore, it is advantageously not compromising the security that the key T is given back from the second device to the first device in a clear form.

[0036] It is emphasized again that the method and system according to the invention can be applied to signing and signature verification accordingly.

[0037] Further features, details and advantages of the present invention will become evident from the following detailed description of embodiments of the invention and the corresponding accompanying drawing.

[0038] In the drawing show:

Fig. 1 a schematic view of a preferred embodiment of the invention together with the

underlying data flow;

Fig. 2a a flow diagram illustrating a method for encryption/decryption according to the invention;

Fig. 2b a flow diagram according to Fig. 2a in case of a signing/signature verification.

[0039] Fig. 1 depicts a scenario where a chip card 1 is inserted in a chip card reader 2 which does not yet have a required software component capable of accessing the chip card 1. Therefore the operating system of the card reader 2 initiates that the missing software component be downloaded 3 from a central server 4 to the card reader 2. In order to validate that the downloaded software component was certified by the issuer and has not been altered in the meantime, in accordance with the invention, the following mechanism is proposed. The issuer's certificate and corresponding private key "I" is stored on the chip card 2 at the time the card is issued. Prior to the software download 3, an encryption with a session key "T" is applied to the underlying software component. The downloaded data therefore contains the cyphered software plus key "T_i", i. e. the key "T" encrypted by a key "I", plus a command (APDU) to trigger or to make the chip card 1 decrypt key "T_i". The APDU command, when sent to the chip card 1, results in a decryption of the key "T_i" to reveal key "T" that was used to encrypt the software component. Due to the above-mentioned combination of two different key levels, the card issuer can every time change key "T" by another random key to encrypt the service with the cryptographic function. Therefore, it is not compromising the security that the key "T" is given back from the chip card 1 to the card reader 2 (terminal device) in clear form. The software module, in this embodiment, is to drive the terminal device 2 to access the chip card 1, but such a software module can also be an application program to run on either the chip card 1 or the terminal device 2 or fulfill specific functions on the terminal device 2 or another (optional) device 5 connected or attached to the terminal device 2. The device 5 can be part of the terminal device and can be any information handling device or system, or only part of such a system like a video display or the like. Normally the terminal device 2 will be a non-intelligent card accepting device and the device 5 an intelligent card reader. Further, the software module can be a driver to drive the chip card or an instrument to control access to the chip card itself.

[0040] It is emphasized that the functionality of the terminal device as proposed by the invention can be implemented by means of common memory and processor hard- and software components.

[0041] The underlying encryption/decryption process consists of the following steps. The information unit s is encrypted by using the key "T" and the key "T" is encrypted by using key "I" as follows:

$$x = \text{enc}(s, T);$$

$$T_i = \text{enc}(T, I).$$

5 [0042] Both "x" and "T_i" are transferred from the central server 4 to the card reader 2. The card reader 2 then instructs the chip card 1 to decrypt "T_i" using "I":

$$T = \text{dec}(T_i, I).$$

10 [0043] The chip card 1 returns the decrypted key "T" to the card reader 2. The card reader 2 uses the key "T" to decrypt the information unit "x":

$$s = \text{dec}(x, T).$$

15 [0044] Fig. 2a depicts a flow diagram illustrating a method for encryption/decryption according to a preferred embodiment of the invention. When the chip card is inserted 20 in the card reader, the card reader firstly checks 21 whether a software support module, e. g. one required to access the chip card or to run a specific function of the chip card on the card reader, or a further device attached to the card reader, is locally available. In case it is 22, it is jumped to step 23 where the available module is executed 23. If the module is not available 24, the card reader builds up an online (telecommunication) connection to the central server and downloads 25 the required module from the server. It should be noted that the download of the module is only an exemplary embodiment i. e. the module can alternatively be provided by the issuer via post mail of a data carrier like a floppy disk. According to the invention, the downloaded module will be in an encrypted format wherein for the encryption an encryption key "T" is used. Together with the support module, the encryption key is downloaded too, but also in an encrypted format "T_i" wherein for the encryption a further encryption key "I" is used. Further an 'APDU' control command is downloaded for activating the chip card to participate in the following decryption process as proposed by the invention. As it is commonly used, the overall package (support module + T_i + APDU) can be downloaded as one file, e. g. in a compressed format using known compression tools like "WINZIP" or "PKZIP".

30 [0045] Then the 'APDU' control command is sent 26 to the chip card in order to initiate or to trigger the chip card to decrypt 27 the encrypted key "T_i" by using key "I". Alternatively the chip card can be initiated to transmit the key "I" to the card reader and the decryption of "T_i" performed by the card reader. In case the chip card fulfills the decryption, the decrypted key "T" will be transferred back 28 to the card reader and then the support module be decrypted 29 by an operating system or program available on the card reader, by using the key "T". The resulting decrypted support module then will be executed 23 by the card reader.

55 [0046] In case of an underlying signature/signature

verification, the mechanism proposed by the invention consists of the following steps. The information unit "s" is signed by using a signature key "I":

$$x = \text{sign}(s, I_{\text{priv}}).$$

[0047] Both "x" and "s" are transferred from the central server 4 to the card reader 2. The card reader 2 then gathers the key "I" for signature verification from the chip card 1 and performs the following signature verification operation:

$$\text{signver}(s, x, I_{\text{pub}}) == \text{OK} ?$$

[0048] A corresponding flow diagram depicted in Fig. 2b shows the proposed mechanism in case of the signing/signature verification instead of the above described data encryption/decryption. As in Fig. 2a, after the chip card is inserted 30 in the card reader, the card reader checks whether a required support module is locally available 31. If so 32, the module is executed 33. If not 34, the required module and the 'APDU' command are downloaded 35 from the central server whereby the module is signed with a private key " I_{priv} ". The 'APDU' command is accordingly sent 36 to the chip card in order to initiate or trigger the chip card to send back 37 a public key " I_{pub} " which is necessary to verify 38 the signature. According to the teaching of the invention, the required public key " I_{pub} " is provided by the chip card itself and transferred to the terminal device at first when having received the 'APDU' command. This key is then used to verify the signature of the downloaded module and in case of a matching signature 39, the software module is executed 33, for instance in order to drive the chip card to execute a particular application either in the chip card or the card reader. If both signatures do not match 40, an error message of the kind 'Invalid Signature' is output by the card reader, e. g. acoustically or by means of a display.

[0049] In cases where the card reader has a secure software execution that only allows code to be executed that was validated by the chip card, i. e. it can not only be ensured that the downloaded software was not altered, but also that the software was certified by the issuer of the card, and that the version of the software is appropriate.

[0050] Thereupon it is secured that the code can only be executed if it was certified by the issuer of the card, the issuer can make sure that the software accessing the card does not make any operations that can insecure the system like sending data to somebody else or logging data.

[0051] For a version control, the following step can be added to the sequence of steps depicted in either Fig. 2a or Fig. 2b:

External authentication with key "E" in order to verify that the version of the software module matches

the smart card.

[0052] Authentication is herein regarded as any process through which one proves and verifies certain information. A chip card commonly uses external authentication to establish the identity of the terminal. This is done by ensuring that the terminal device shares a secret with the chip card.

[0053] An external authentication starts with the chip card wondering about the terminal's identity and sending a challenge - for example a random 8-byte sequence - to the terminal whose identity is being questioned. The terminal receiving the challenge encrypts it with its secret, a particular key, and sends back the encrypted result. The chip card now decrypts the encrypted message using the key it knows the terminal possesses if it is authentic. If the message decrypts satisfactorily, i. e. the decrypted challenge is identical to the challenge originally sent by the chip card, then the chip card knows that the terminal possesses a particular key and this establishes its identity.

Claims

1. A method for securely handling an information unit by a first information processing device (2) inter-operating with a second secure information processing device (1), in particular a chip card, whereby the information unit is provided by an issuer, the method being characterized by the steps:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being processed by a cryptographic process;

providing at least one key for the cryptographic process on the second secure information processing device (1);

cryptographically reprocessing (29, 38) the information unit by using the at least one key.

2. Method according to claim 1, characterized by the particular steps:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being encrypted by using at least a first key;

providing the first key from the issuer to the first information processing device (2), the first key being encrypted by using at least a second key;

providing the at least one second key on the second secure information processing device (1);

interconnecting the first information processing device (2) and the second secure information processing device (1);

on side of the second secure information processing device, decrypting (27) the at least first key by using the at least second key;

decrypting (29) the information unit by using the decrypted at least first key.

3. Method according to claim 1, characterized by the particular steps:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being signed by using a signature;

providing the signature from the issuer to the first information processing device (2), the signature being generated by using at least one key;

providing the at least one key for signature verification on the second secure information processing device (1);

interconnecting the first information processing device (2) and the second secure information processing device (1);

transferring the at least one key for signature verification from the second secure information processing device to the first information processing device;

verifying the signature of the information unit by using the at least one key.

4. Method according to claim 1 or 2, characterized in that the decrypted at least first key is transferred to the first information processing device (2) and the information unit is decrypted (29) on side of the first device (2).

5. Method according to one or more of the preceding claims, characterized in that the first information processing device (2) provides a control command (26, 36) to the second secure information processing device (1) to initiate decryption of the at least first key by using the at least second key and/or to initiate transferring the signature key for signature verification from the second secure device to the first device.

6. Method according to one or more of the preceding claims, characterized in that the encrypted informa-

tion unit, the encrypted first key, and/or the signature key, and/or the generated signature, and/or the control command are downloaded (25, 35) from a central server (4).

7. Method according to one or more of the preceding claims, characterized in that the second key and/or the key for signature verification are/is securely stored on the second secure device (1) at time of its issuing by the issuer.

8. Method according to one or more of the preceding claims, characterized in that providing at least a third key for external authentication and/or release control of the respective information unit.

9. Method according to claim 8, characterized in that the first device (2) is initiated to gather a new release of the information unit from the issuer, depending on the respective status of the third key.

10. Method according to claim 9, characterized in that the new release of the information unit is downloaded from an internet server (4) provided by the issuer.

11. Method according to one or more of the preceding claims, characterized in that the at least first key and/or the signature are/is randomized between different sessions of providing the information unit from the issuer to the first device (2).

12. Method according to one or more of the preceding claims, characterized in that the first information processing device (2) being a terminal device, in particular a chip card reader, and the second secure information processing device (1) being a portable device, in particular a chip card.

13. A system for securely handling an information unit, comprising a first information processing device (2) interoperating with a second secure information processing device (1), in particular a chip card, the information unit being provided by an issuer, characterized in that

the first device (2) comprises

a storage for storing the information unit;

the second secure device (1) comprises

a storage (6) for storing at least one key for a cryptographic process;

providing means for cryptographically reprocessing the information unit by using the at least one key.

14. System according to claim 13, characterized in that
- the first device (2) comprises
- a storage for storing the information unit, encrypted by using at least a first key, and a storage for storing the first key, encrypted by using at least a second key;
- the second secure device (1) comprises
- a storage (6) for storing the at least one second key, and processing means for decrypting the at least first key by using the at least second key;
- providing means for decrypting the information unit by using the decrypted at least first key.
15. System according to claim 13, characterized in that
- the first device (2) comprises
- a storage for storing the information unit and a signature for the information unit;
- the second secure device (1) comprises
- a storage (6) for storing at least one signature key;
- providing means for verifying the signature of the information unit by using the at least one signature key.
16. System according to one or more of claims 13 to 15, characterized in that the second secure device (1) provides an access control by means of the information unit.
17. System according to one or more of claims 13 to 16, characterized in that the second secure device (1) comprises a processor to make specific functions of the second secure device usable/accessible on the first device or on at least a third device (5) attached to the first device.
18. System according to one or more of claims 13, 14, 16 or 17, characterized in that the first device (2) comprises processing means for decrypting (29) the information unit by use of the decrypted at least first key.
19. System according to one or more of claims 13 to 18, characterized in that the second secure device (1) comprises means to initiate decryption of the at least first key by using the at least second key and/or means to initiate transfer of the signature key for signature verification from the second secure device to the first device.
20. System according to one or more of claims 13 to 19, characterized in that the first device (2) comprises means to download the encrypted information unit, the encrypted first key, and/or the generated signature, and/or the control command, from a central server (4).
21. System according to one or more of claims 13 to 20, characterized in that the second secure device (1) comprises a non-erasable storage to store the second key and/or the signature key at time of its issuing.
22. System according to one or more of claims 13 to 21, characterized in that the first device (2) and/or the second secure device (1) comprise/s a storage (6) for storing at least a third key for external authentication and/or release control of the information unit and processing means (7) for processing the third key.
23. System according to one or more of claims 13 to 22, characterized in that the first device (2) comprises means to initiate download of a new release of the information unit, depending on the respective status of the third key.
24. System according to one or more of claims 13 to 23, characterized in that the central server (4) comprises a randomizer for randomizing the at least first key and/or the signature between different sessions of providing the information unit from the issuer to the first device.
25. System according to one or more of claims 13 to 24, characterized in that the first information processing device (2) being a terminal device, in particular a chip card reader, and the second secure information processing device (1) being a portable device, in particular a chip card.
26. A chip card (1) for securely handling an information unit by interoperating with an information handling terminal device (2), characterized in that using a method according to one or more of claims 1 to 12 and/or being usable in a system according to one or more of claims 13 to 25, whereby comprising a storage (6) for storing the at least one key for the cryptographic process.
27. Chip card according to claim 26, characterized by processing means (7) performing an access control controlled by the information unit.
28. Chip card according to claim 26 or 27, character-

ized by a processor (7) to run specific functions on the terminal device (2, 5) or on at least a second device attached to the terminal device (2, 5).

29. Chip card according to one or more of claims 26 to 28, characterized by means for transferring of the at least one second key to the terminal device (2, 5) and/or means for decrypting of the at least first key by using the at least second key and/or means to initiate transfer of the signature key for signature verification. 5 10
30. Chip card according to one or more of claims 26 to 29, characterized by a non-erasable storage (6) to store the second key and/or the signature key at time of its issuing. 15
31. Chip card according to one or more of claims 26 to 30, characterized by a storage (6) for storing at least a third key for external authentication and/or release control of the information unit and processing means (7) for processing the third key. 20
32. Chip card according to claim 31, characterized by processing means (7) to initiate download of a new release of the information unit, depending on the respective status of the third key. 25
33. A chip card accepting device (2), in particular a chip card reader, for securely handling an information unit by interoperating with a chip card (1), **characterized in that** using a method according to one or more of claims 1 to 10 and/or being usable in a system according to one or more of claims 13 to 25 and/or being usable for a chip card (1) according to one or more of claims 26 to 32, whereby comprising a storage for storing the information unit. 30 35
34. Chip card accepting device according to claim 33, characterized by means for decrypting the information unit by using at least one key. 40
35. Chip card accepting device according to claim 33 or 34, characterized by means for verifying a digital signature. 45
36. Chip card accepting device according to one or more of claims 33 to 35, characterized by means for downloading the encrypted information unit, the at least one key and the digital signature from a central server (4). 50
37. Chip card accepting device according to one or more of claims 33 to 36, characterized by a storage for storing at least a third key for external authentication and/or release control of the information unit and processing means for processing the third key. 55
38. Chip card accepting device according to one or more of claims 33 to 37, characterized by means to initiate download of a new release of the information unit, depending on the respective status of the third key.

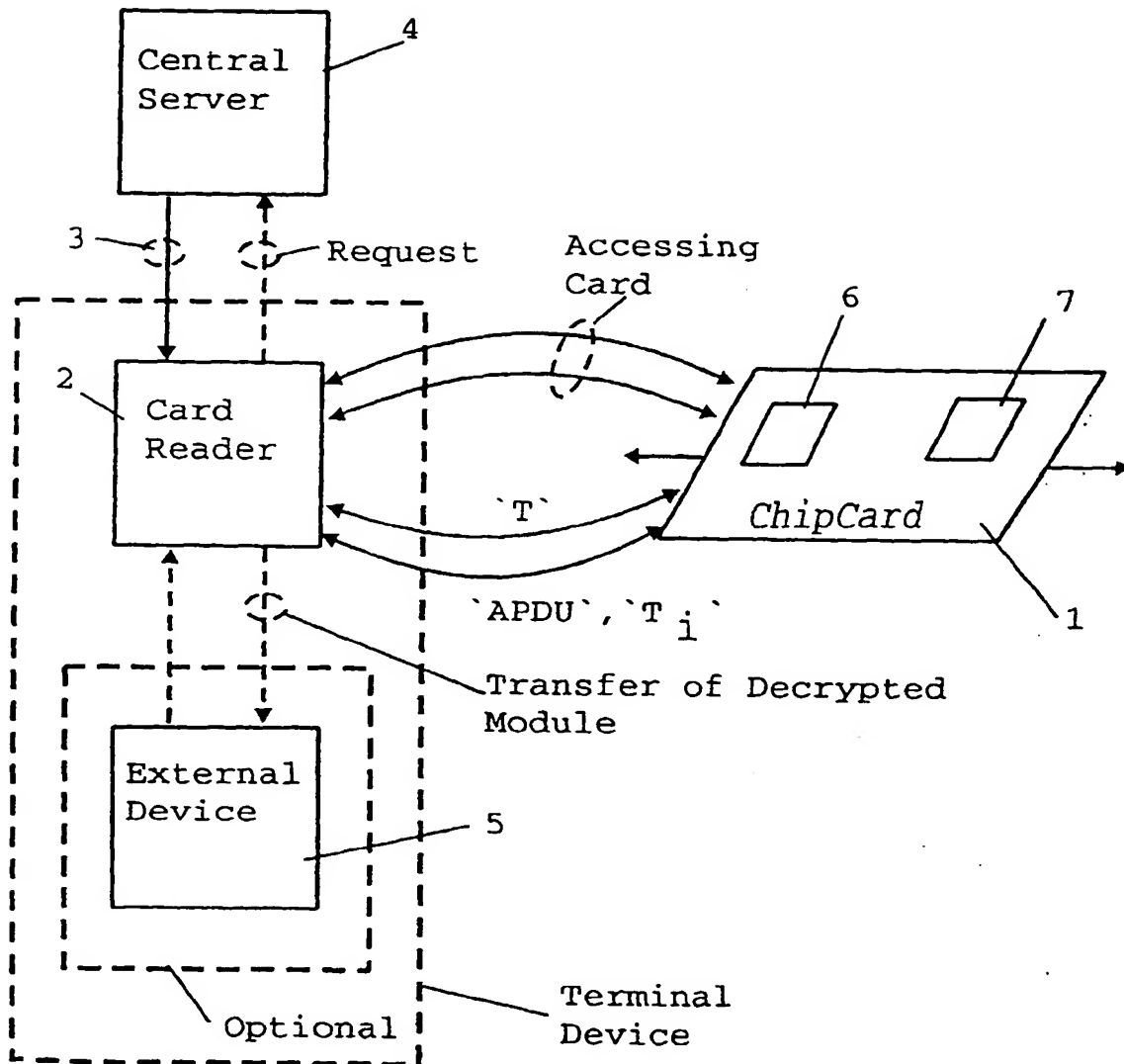


FIG. 1

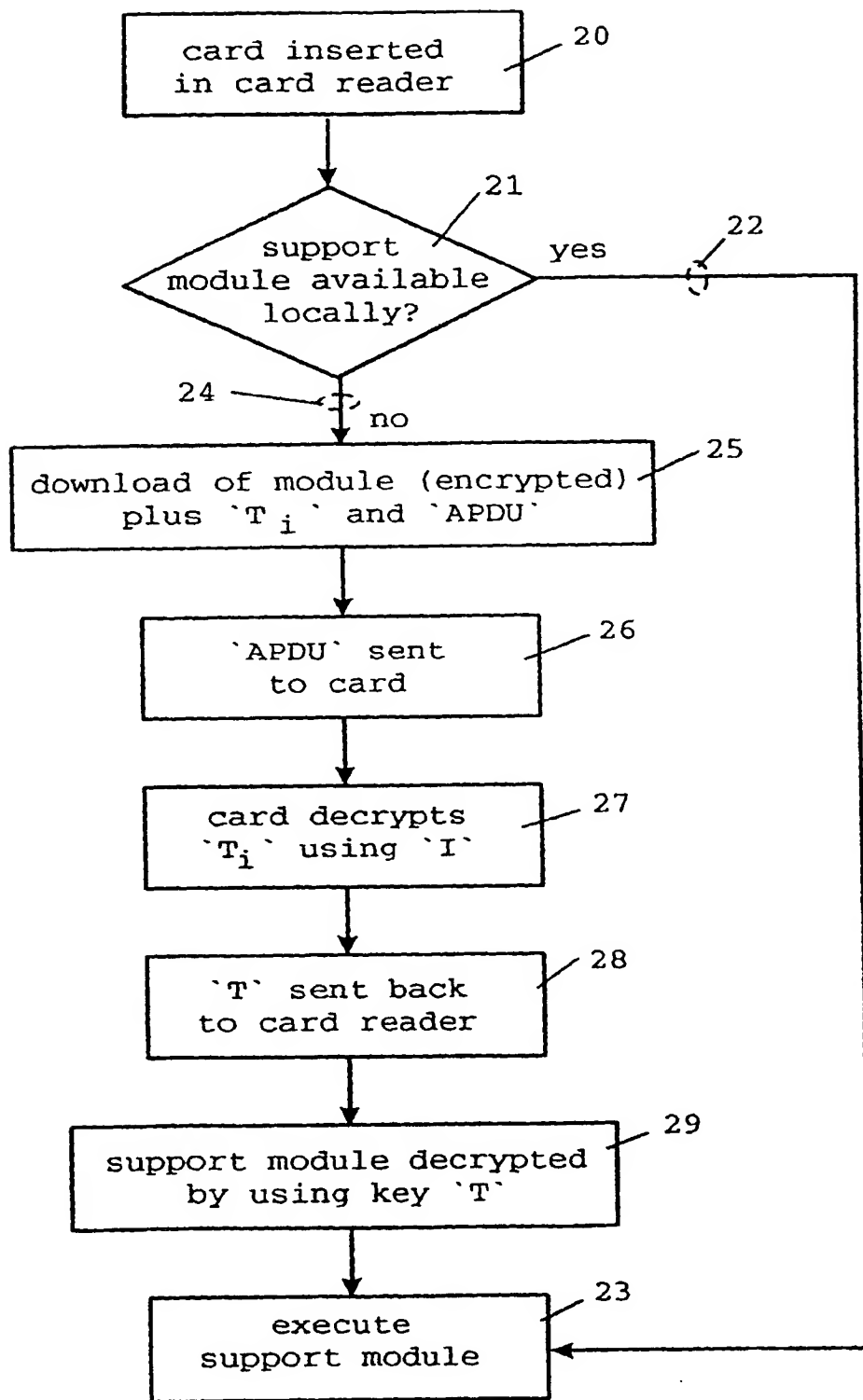


FIG. 2A

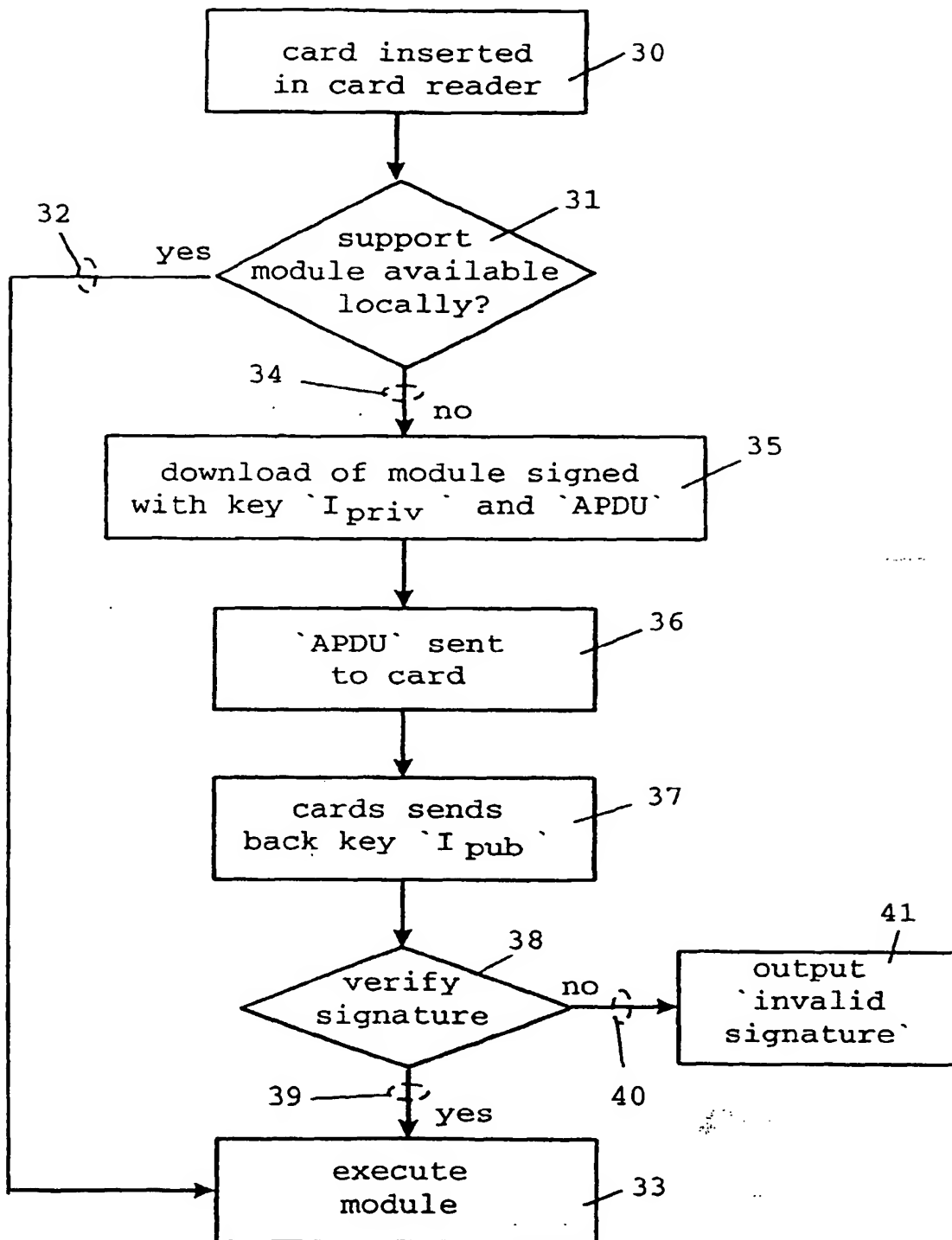
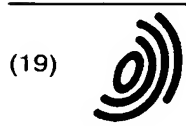


FIG. 2B

THIS PAGE BLANK (USPTO)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 1 022 638 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
02.05.2001 Bulletin 2001/18

(51) Int. Cl.⁷: G06F 1/00

(43) Date of publication A2:
26.07.2000 Bulletin 2000/30

(21) Application number: 00100476.1

(22) Date of filing: 11.01.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 12.01.1999 EP 99100474

(71) Applicant:
International Business Machines Corporation
Armonk, NY 10504 (US)

(72) Inventors:
• Hansmann, Uwe
71155 Altdorf (DE)
• Seliger, Frank
71157 Hildrizhausen (DE)

(74) Representative:
Teufel, Fritz, Dipl.-Phys. et al
IBM Deutschland Informationssysteme GmbH,
Intellectual Property,
Pascalstrasse 100
70548 Stuttgart (DE)

(54) Method and system for securely handling information between two information processing devices

(57) Described is a mechanism for securely handling an information unit by a first information processing device (2), for instance a terminal device like a chip card reader, which interoperates with a second secure information processing device (1), for instance a portable device like a chip card, whereby the information unit is provided by an issuer. The information unit is provided from the issuer to the first device and encrypted by using a first key. The first key is also encrypted by using a second key. The second key is provided on the second secure device (1) and interconnecting the first and the second device enables to decrypt the first key by using the second key and then to decrypt the information unit by using the first key.

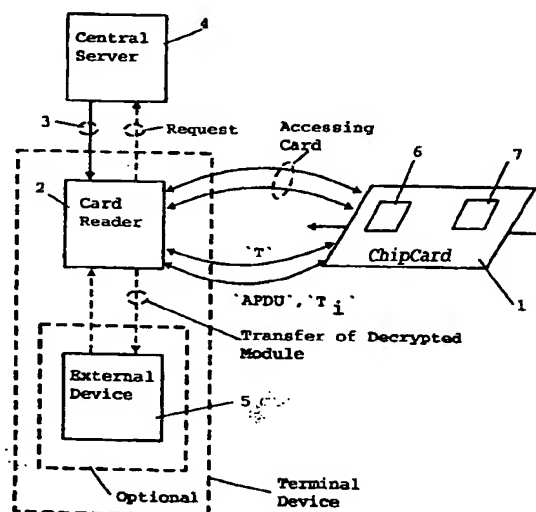


FIG. 1

EP 1 022 638 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 10 0476

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 98 03904 A (HAGLUND MAGNE ARILD; SIGBJOERNSEN SIGURD (NO); OLESHCHUK VLADIMIR) 29 January 1998 (1998-01-29) * abstract; figure 6 * * page 3, line 33 - page 5, line 9 * * page 6, line 7 - line 17 * * page 9, line 13 - page 11, line 31 * * page 13, line 9 - page 5, line 10 *	1,2,4,5, 12,13, 25,26,33	G06F1/00
Y	---	3,7,15	
X	EP 0 715 242 A (NIPPON TELEGRAPH & TELEPHONE) 5 June 1996 (1996-06-05) * abstract; figures 1,3,4 * * column 2, line 3 - line 49 * * column 11, line 52 - column 13, line 6 *	1,2,4-6, 12-14, 18-20, 25,26, 29,33-36	
Y	---	3,7,11, 15,21, 24,30	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
Y	US 5 689 565 A (SPELMAN JEFFREY F ET AL) 18 November 1997 (1997-11-18) * abstract; figure 10 * * column 17, line 49 - line 63 *	11,24	G06F
Y	DE 197 08 616 A (SIEMENS AG) 17 September 1998 (1998-09-17) * abstract; figure 1 * * column 4, line 53 - line 56 *	21,30	

-The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 23 November 2000	Examiner Sigolo, A
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03.92 (P04C01)



European Patent
Office

Application Number

EP 00 10 0476

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

- ☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):
- ☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

- ☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.
- ☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.
- ☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:
- ☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:
- 1-7, 11-15, 18-21, 24-26, 29, 30, 33-36



European Patent
Office

**LACK OF UNITY OF INVENTION
SHEET B**

Application Number
EP 00 10 0476

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1-7, 11-15, 18-21, 24-26, 29,30, 33-36

Method, system, chip card and chip card accepting device for securely handling an information unit against tampering, where security control is cooperatively performed by the chip card and the chip card accepting device using decryption or alternatively signature verification.

2. Claims: 8-10, 22,23, 31,32, 37,38

Method, system, chip card and chip card accepting device for securely handling an information unit against tampering, where security control is cooperatively performed by the chip card and the chip card accepting device using decryption.

Method, system, chip card and chip card accepting device further comprising verification of the information unit version.

3. Claims: 16,17,27,28

System and chip card for securely handling an information unit against tampering, where security control is cooperatively performed by the chip card and the chip card accepting device using decryption.

System and chip card further comprising access control provided by the chip card by means of the information unit.

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 10 0476

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-11-2000

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9803904	A	29-01-1998	NO	962997 A	19-01-1998
			AU	3466997 A	10-02-1998
EP 0715242	A	05-06-1996	JP	8160855 A	21-06-1996
			JP	8160856 A	21-06-1996
			US	5701343 A	23-12-1997
US 5689565	A	18-11-1997	NONE		
DE 19708616	A	17-09-1998	BR	9808167 A	16-05-2000
			CN	1254421 T	24-05-2000
			WO	9839701 A	11-09-1998
			EP	0965076 A	22-12-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)